

REMARKS

Applicants reply to the Final Office Action dated August 19, 2008 within three months. Claims 1-50 were pending in the application and claims 1, 14, 26 and 37 are independent. The Examiner rejects claims 1-50. Support for the amendments may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments. Applicants respectfully submit that the application is in condition for allowance and request reconsideration of the pending claims.

As an initial matter, Applicants note that the terms “contents encryption device” and “contents decryption device” were recited in claims 5, 12 and 50. Applicants amend such recitations to “encryption device” and “decryption device”, respectively, for consistency of claim language.

The Examiner rejects claims 1-50 under 35 U.S.C. §112 as failing to comply with the written description requirement. Applicants respectfully traverse this rejection, but in the interest of compact prosecution, Applicants amend the claims to remove the rejected language.

The Examiner finds the Applicant’s argument directed to the lack of support rejection for the feature “contents decryption key is not required to be encrypted or decrypted by the contents decryption device” to be unpersuasive. In particular, the Examiner requires explicit support from the specification, noting that such a feature is based on a negative requirement. Therefore, the Examiner maintains his lack of support rejection for such a feature.

Applicants respectfully disagree with the Examiner’s rejection, so Applicants provide an explanation of how such a feature should be correctly interpreted by one of ordinary skill in the art. Firstly, from the specification of the subject application it should be clearly understood by one of ordinary skill in the art that the contents keys CK do not have to be transferred. Referring to Figure 1, encryption device 101 and decryption device 102 each have a corresponding contents key generations section (117, 118). Support can be found on page 25, lines 10-20 of the English language specification. In the present Office Action, section 4 paragraph 3, the Examiner correctly notes that it is the decryption limitations which are transferred in the present invention. Transferring the actual key and transferring the elements which the key is based on are very different features. For example, the key can be generated after the elements which the key is based on are transferred. As such, it follows that encrypting a key and encrypting the elements used to generate a key are different as well. Therefore, it is inappropriate for the

Examiner to correlate an encrypted key being transferred to be the same as the encrypted elements, which the key is based on, being transferred.

Since it is clear from the disclosure of the present application that the keys themselves do not have to be transferred, it is also understood that no such encryption of the keys would be required as well. This is because the point of encryption is for security reasons during transfer. A key local to the device would hence not need to be encrypted.

Regarding the lack of support rejection detailed in section 7.3 of the last Office Action, the Examiner has withdrawn the lack of support rejection regarding the feature “time-varying keys not required to be transmitted”, alleging that the Applicant has admitted such a feature to be prior art, as suggested by the Examiner in the last Office Action. Subsequently, the Examiner has withdrawn this rejection as no explicit disclosure is necessary for such a feature. However, Applicants have not admitted to such a fact. In particular, Applicants stated that one of ordinary skill in the art would understand the disclosure of the present application to support such a feature. Similar to the arguments presented above, the specification of the present application discloses that same time-varying keys VK are generated in a time-varying key generation section 113, 114 in both the encryption device 101 and decryption device 102. Thus, since the same keys are generated in each of the encryption and decryption devices, the keys do not have to be transferred between the devices and transferring such keys would serve no purpose. Rather, the present invention teaches transferring random numbers R1, R2 and response values V1, V2 to generate the time-varying keys in each device. See page 23, line 28 to page 26, line 26 of the English specification of the present application.

Therefore, although Applicants agree that such a rejection should be withdrawn, Applicants assert that such a rejection should be withdrawn due to the disclosure of the present application and not because Applicants admit such feature to be prior art.

The Examiner next rejects claim 1 under 35 U.S.C §103(a) as being obvious over Ishibashi (USP 6,728,379). The Examiner also rejects claims 2-50 under 35 U.S.C §103(a) as being obvious over Ishibashi (USP 6,728,379) and further in view of Frutiger (USP 4,071,693). Applicants respectfully traverse these rejections, but in the interest of compact prosecution, Applicants amend the claims as set forth herein and provide the following remarks.

The Examiner asserts that the decryption device of Ishibashi also does not decrypt the keys as recited in the presently claimed invention. In addition, the Examiner also asserts that the invention of Ishibashi also teaches transferring key elements and generating the key at the

device. The Examiner notes that if encryption and decryption of the final key is not required in the Applicant's invention, the same applies to the invention disclosed by Ishibashi. Moreover, the Examiner alleges that since Ishibashi's invention relates to controlling the number of copies made available to the user and that profits are shared with the content provider based on the copies purchased by a user, there is a level of cooperation between the user side and the content provider. Lastly, the Examiner asserts that key encryption corresponds to key generation. Thus, the information processor of Ishibashi's invention also performs key generation. In view of the above, the Examiner concludes that the claimed invention of claim 1 is still not inventive over the disclosure of Ishibashi.

Applicants respectfully assert that the Examiner's comments are contrary to an understanding of the intent of the presently claimed invention. Nonetheless, to expedite prosecution, Applicants amend the pending claims to further define the generation of the contents key based on an updated decryption limitation in the decryption device.

Amended claim 1 recites:

“wherein the decryption device includes
a second contents key generation section for generating the
contents decryption key from the second decryption limitation, the
second decryption limitation obtained by updating the first
decryption limitation in the decryption device, and
a first decryption section for decrypting the encrypted
contents transferred from the encryption device using the contents
decryption key generated by the second contents key generation
section” (emphasis added)

Support for this amendment can be found in at least page 24, lines 28-33 and page 25, lines 16-20. Independent claims 26 and 37 recites a similar feature while independent claim 14 is the related encryption device and thus not appropriate for such amendment.

Applicants assert that Ishibashi fails to teach or suggest the aforementioned features. In particular, referring to Figure 8, Ishibashi teaches that an encrypted content decryption key **Kde(Kcd)** is decrypted by a distribution key **Kdd** in the content key decrypt section 131 of information processor 100 to generate content key **Kcd**. See col.10. lines 27-33 of Ishibashi. Subsequently, the information processor 100 decrypts the encrypted content **Kce(Cont)** transferred from the content provider 10 with the content decryption key **Kcd** in the content key

decrypt section 136. See col.10, lines 52-55. The content key is then encrypted with an updated copy control code in the content key encrypt section 133 generating the content key **Kcd^{ex}**. See col.11, lines 5-9. In addition, see the process described from col.11 line 56 to col.12, line 15, which clearly describes that the content is decrypted by **Kcd** before the copy control code is updated. Thus, the content key used to decrypt the encrypted data is not generated prior to the decryption limitation being updated. This is different because the presently claimed invention includes the content key used to decrypt the encrypted content transferred from the encryption device be generated based on an updated decryption limitation.

Applicants assert that neither keys **Kcd** nor **Kcd^{ex}** correspond to such a key. In particular, content key **Kcd** is used to decrypt the encrypted content transferred from the encryption device but is not generated based on the updated copy control code. On the other hand, content key **Kcd^{ex}** is generated based on the updated copy control code but does not decrypt the encrypted content transferred from the encryption device, but rather is sent to a destination apparatus. See col.12, lines 32-34.

Advantageously, since the content keys of both the encryption and decryption device are generated based on an updated decryption limitation, the encrypted contents provided cannot be decrypted unless the decryption limitation is updated in an authorized manner as discussed above. Thus, Applicants assert that an intent of the invention is that the content keys be generated based on an updated decryption limitation before it decrypts the encrypted content. See page 26, lines 20-26 of the English language specification.

For at least these reasons, Applicants assert that the claimed invention is novel and inventive over Ishibashi. In addition, Frutiger does not make up for these deficiencies of Ishibashi as it only relates to time-varying keys. Accordingly, the present obviousness rejection should be withdrawn with respect to the present claims.

The Examiner asserts that the presently claimed invention corresponds with the invention of Ishibashi. Applicants respectfully disagree and set forth the following analysis of the significant differences between teachings of Ishibashi and the presently claimed invention.

In the presently claimed invention, two of the main components are the encryption device 101 and the decryption device 102. The Examiner asserts that the encryption device can correspond to either the content provider 10 or the information processor 100. Therefore, there are two cases to consider.

(case 1)

In the case that the encryption device is considered to be the content provider 10, then the information processor 100 is considered to be the decryption device. The below discussion refers to Figure 8 of Ishibashi.

Encryption (content provider 10)

The content provider 10 generates a content encryption key **Kce** and a content decryption key **Kcd**. The content encryption key **Kce** is used to encrypt the desired content into encrypted content **Kce(Cont)** and the content decryption key **Kcd**, used to decrypt the encrypted content **Kce(Cont)** in the information processor 100, is encrypted by a distribution encryption key **Kde** into encrypted content decryption key **Kde(Kcd)**. Then the content provider 10 transmits the encrypted content **Kce(Cont)** and the encrypted content decryption key **Kde(Kcd)** to the information processor 100. See col.8, line 39 to col.9, line 10.

Decryption (information processor 100)

The information processor 100 receives the encrypted content **Kce(Cont)** and encrypted content decryption key **Kde(Kcd)** and stores it in the HDD 110. The information processor 100 further receives the distribution decryption key **Kdd**. The distribution decryption key **Kdd** and encrypted content decryption key **Kde(Kcd)** are sent to the content key decryption section 131 where the former is used to decrypt the latter. The decrypted content decryption key **Kcd** is then used to decrypt the encrypted content **Kce(Cont)** at the content decryption section 136, is provided a changed copy control code in the copy controller 137, and encrypted to include a copy control code provided by the copy controller 137 by a session key **Ksession** in the content key encryption section 133. See col. 9. line 53 to col.11. line 16 of Ishibashi.

Deficiencies (present invention vs Ishibashi)

In this case, at least the following deficiencies exist.

Firstly, the content provider 10 does not contain a decryption section as include by the encryption device of the claimed invention, as recited in claim 2 for example.

Secondly, the content provider 10 has not been described to contain the decryption limitation as disclosed in the presently claimed application, since the content provider has not been described to include copy control code.

The Examiner argues that it would be obvious to generate the content decryption key **Kcd** based on copy control code, as described for information processor 100, in the content provider 10, since the invention of Ishibashi is related to controlling the number of copies of

content. However, Applicants strongly disagree and Applicants believe that it would be an inappropriate assertion, in view of the disclosure of Ishibashi.

As previously argued and not addressed by the Examiner in the present Office Action, control of copies of content is already accounted for by the copy controller. It is unclear why updated copy control code in the decryption device, information processor 100 which is on a user-side, should influence the encryption device, content provider 10 which is on a server-side. It would be illogical for an updated copy control code of content already provided to a user to have any effect on the copy control code of new content and content keys to be provided to another user in the content provider 10. Applicants respectfully assert that the Examiner has merely said that there would be cooperation between server side 10 and the user side 100, but has failed to clearly indicate the specifics of such cooperation. See page 5, paragraph 2 of the present Office Action. Applicants respectfully request the Examiner to explicitly provide the specifics of such cooperation.

Even though the Examiner has not provided specific details on specifically how the content provider 10 would incorporate such a feature of the information processor 100, Applicants set forth the below analysis of how such a combination would be interpreted by one of ordinary skill in the art.

In particular, Ishibashi teaches for the information processor 100, that a copy control code, corresponding to a decryption limitation, be encrypted into a content decryption key to reduce labor, although it can be encrypted into content as well. See col.6, lines 1-19 of Ishibashi. As such, the copy control code is taught to be encrypted with a content decryption key and transferred to decrypt corresponding encrypted content. The content decryption key is used to decrypt the encrypted content and the copy control code is subsequently updated when the content is decrypted.

If this disclosure is applied to the content provider 10, this would result in the content decryption key **Kcd** being encrypted with a copy control code and associated with a corresponding encrypted content **Kcd(Cont)**. The encrypted content decryption key with the copy control code **Kcd** and the encrypted content **Kcd(Cont)** would be transferred to the information processor 100. Subsequently, the encrypted decryption key having the copy control code would be decrypted and used to decrypt the corresponding encrypted content. The copy control code would be updated and encrypted back to the content encryption key.

However, the presently claimed invention clearly includes that the decryption limitation be updated before the content keys in the encryption and decryption devices are generated. The content keys are then generated based on the updated decryption limitation. Ishibashi does not disclose or contemplate such a feature. In contrast, the invention of Ishibashi as discussed above would teach that the content be encrypted and decrypted by a content key generated by a decryption limitation (copy control code) before the limitation is updated. Thus, the disclosure of Ishibashi cannot teach generating a content key based on an updated decryption limitation even when considering the description of the information processor 100 being applied to the content provider 10.

The Examiner may assert that the information processor 100 teaches encrypting a content decryption key **Kcd** with an updated copy control code into **Kcd^{cx}** and thus a content key based on an updated encryption limitation is generated. However, such an assertion would be inappropriate because the presently claimed invention includes that the content key generated based on an updated encryption limitation in the decryption device is used to decrypt the encrypted data provided by the encryption device, which is not done by key **Kcd^{cx}**. Moreover, the encryption device generates a content key based on an updated encryption limitation, which is not disclosed nor contemplated. Thus, neither of the content keys **Kcd** nor **Kcd^{cx}** generated in the information processor 100 discloses the content key of the presently claimed invention.

Lastly, the claimed invention clearly includes that the same time-varying key to be used to encrypt and decrypt the decryption limitations in the encryption and decryption device. However, Ishibashi teaches that the content provider 10 only encrypts the elements used to generate the contents key using the distribution key **Kde**. The content provider 10 does not decrypt any elements. In addition, the information processor 100 decrypts the elements, **Kcd** or the copy control code, using the distribution key **Kdd** but encrypts the updated elements, **Kcd^{cx}**, using the common session key **Ksession**. Therefore, Ishibashi cannot disclose using the same time-varying key for encrypting and decrypting the decryption limitations in both the encryption and decryption devices.

(case 2)

In the case that the encryption device is considered to be the information processor 100, then the information processor 200 is considered to be the decryption device. The below discussion refers to Figure 8 of Ishibashi.

Encryption (information processor 100)

Since the information processor 100 was described in the above section Decryption (information processor 100), such a description will be omitted in this section.

Decryption (information processor 200)

The information processor 200 receives the encrypted content **Kce(Cont)** and encrypted updated content decryption key **Ksession(Kcd^{cx})**. The information processor 200 further receives the session key **Ksession**. The session key **Ksession** and encrypted updated content decryption key **Ksession(Kcd^{cx})** are sent to the content key decryption section 231 where the former is used to decrypt the latter. The decrypted content decryption key **Kcd^{cx}** is then used to decrypt the encrypted content **Kce(Cont)** at the content decryption section 236 and is provided a updated copy control code in the copy controller 237. It is also described that such features are the minimum necessary components and may have all the functions of information processor 100. See col. 11, lines 17-36 of Ishibashi.

Deficiencies (present invention vs Ishibashi)

In this interpretation, there are at least the following deficiencies.

Firstly, the information processor 100 does not encrypt contents, it only decrypts contents. The information processor 100 merely stores encrypted contents **Kce(cont)** provided by a content provider 10 in the HDD 110. See col.8, lines 8-13 of Ishibashi. The presently claimed invention includes that the encryption device to encrypt contents as recited in claim 1 “a first encryption section for encrypting the contents . . .”.

Secondly, regarding the elements which correspond to the decryption limitations of the presently claimed invention, since the copy control code is updated, this should correspond to the decryption limitations. However, in the information processor 100, the encrypted content key **Kde(Kcd)** is decrypted by the distribution key **Kdd**. That is, the content key **Kcd** is generated based on distribution key Kdd. Therefore, the content key is not generated based on the decryption limitation, corresponding to the copy control code.

The Examiner may assert that the content key **Kcd^{cx}** is generated in the content key encrypt section 133 based on the updated copy control code from the copy controller 137. However, Applicants respectfully assert that this is clearly inappropriate because the presently claimed invention includes that the content key of the encryption device be generated based on an updated decryption limitation and used to encrypt the contents. As stated above, the information processor 100 does not encrypt contents and thus cannot teach generating a key to

encrypt the contents. In contrast, the content key **Kcd^{cx}** of Ishibashi is only transmitted and used for decrypting in an external apparatus.

Furthermore, as argued above regarding case 1, the presently claimed invention includes that the decryption limitation be updated before the content keys in the encryption and decryption devices are generated. The content keys are then generated based on the updated decryption limitation. The Examiner may assert that the information processor 200 decrypts the encrypted updated content decryption key **Ksession(Kcd^{cx})** transferred from the information processor 100 and thus also generates a content key **Kcd^{cx}** based on an updated decryption limitations. However, the presently claimed invention clearly specifies that the content key of the decryption device is generated based on a decryption limitation which is updated in the decryption device. This content key is then used to decrypt the content. **Kcd^{cx}** does not correspond to such a key because it was not generated based on a decryption limitation updated in the decryption device. In addition, the copy control code is updated in the copy controller 237 after the encrypted contents have been decrypted. Thus, Applicants respectfully assert that such a correspondence is also clearly inappropriate.

Moreover, in the information processor 200, the encrypted updated content key **Ksession(Kcd^{cx})** is decrypted based on the session key **Ksession**. Therefore, the content key **Kcd^{cx}** used to decrypt the encrypted content **Kce(Cont)** is generated based on **Ksession** and not the copy control code. Thus, the content key of the decryption device is not generated based on the decryption limitation, let alone the updated decryption limitation as included in the presently claimed invention.

Thus, it can be seen from case 2 that there are many deficiencies between the invention of Ishibashi and the presently claimed invention.

In view of the above discussion, Applicants respectfully assert that the Examiner is clearly using impermissible hindsight and the Applicant's invention as a template to pick and choose features without considering the invention of Ishibashi as a whole. In particular, it is inappropriate to take features from the information processor and merely say that such feature would be obvious to be included in the content provider. This would be substantially changing the intent of the invention disclosed in Ishibashi. As such, Applicants assert that cases 1 and 2 should be considered separately.

Because many deficiencies exist in both cases 1 and 2 in the correspondence of the invention of Ishibashi with that of the presently claimed invention, it would take substantial

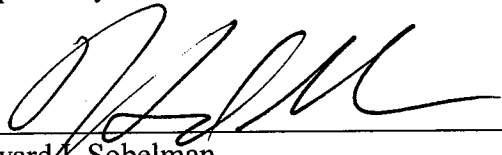
modification to the invention of Ishibashi to arrive at the presently claimed invention. Thus, Applicants strongly assert that such changes are not trivial nor obvious. Importantly, as seen in both case 1 and case 2, Applicants assert that Ishibashi fails to disclose at least the feature of “generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation” which has been further clarified in amended claim 1. Therefore, for at least the reasons discussed above, the present obviousness rejections should be withdrawn.

Claims 2-13, 15-25, 27-36 and 38-50 variously depend from independent claims 1, 14, 26 and 37, so Applicants assert that claims 2-13, 15-25, 27-36 and 38-50 are differentiated from the cited references for the same reasons as set forth above for differentiating independent claims 1, 14, 26 and 37, in addition to their own respective features.

In view of the above remarks, Applicants respectfully submit that all pending claims properly set forth that which Applicants regard as their invention and are allowable over the cited reference. Accordingly, Applicants respectfully request allowance of the pending claims. The Examiner is invited to telephone the undersigned at the Examiner’s convenience if it would help further prosecution of the subject Application. The Commissioner is authorized to charge any fees due to Deposit Account No. 19-2814.

Respectfully submitted,

Dated: November 17, 2008


Howard I. Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com